Парламентское собрание Союза Беларуси и России

Постоянный Комитет Союзного государства

Оперативно-аналитический центр
при Президенте Республики Беларусь

Государственное предприятие «НИИ ТЗИ»

Полоцкий государственный университет

КОМПЛЕКСНАЯ ЗАЩИТА ИНФОРМАЦИИ

Материалы XXII научно-практической конференции

(Полоцк, 16–19 мая 2017 г.)

Новополоцк
2017

УДК 004(470+476)(061.3)
ББК 32.81(4Беи+2)
К63

К63 **Комплексная защита информации :** материалы XXII науч.-практ. конф., Полоцк, 16–19 мая 2017 г. / Полоц. гос. ун-т ; отв. за вып. С. Н. Касанин. – Новополоцк : Полоц. гос. ун-т, 2017. – 282 с.
ISBN 978-985-531-564-4.

В сборнике представлены доклады ученых, специалистов, представителей ггосударственных органов и практических работников в области обеспечения информационной безопасности Союзного государства по широкому спектру научных напрвлений.

Адресуется исследователям, практическим работникам и широкому кругу читателей.

Тексты тезисов докладов, вошедших в настоящий сборник, представлены в авторской редакции.

УДК 004(470+476)(061.3)
ББК 32.81(4Беи+2)

ISBN 978-985-531-564-4

коммуникационных технологий на 2011 - 2015 годы», Национальный реестр правовых актов Республики Беларусь, 30.03.2011, № 5/33546.

3. Постановление Совета Министров Республики Беларусь от 09.08.2011 № 1074 «Об оказании электронных услуг и реализации государственных функций в электронном виде посредством общегосударственной автоматизированной информационной системы», Национальный реестр правовых актов Республики Беларусь, 11.08.2011, № 5/34288.

О ПОДХОДАХ К ОЦЕНКЕ БЕЗОПАСНОСТИ ТЕХНОЛОГИИ БЛОКЧЕЙН

С.Е. КУЗНЕЦОВ, С.В. МАТВЕЕВ

Пензенский филиал Федерального государственного унитарного предприятия «Научно-технический центр «Атлас»

В настоящее время большое внимание уделяется технологии цепной записи данных и распределенных реестров (блокчейн). Технология цепной записи данных и распределенных реестров, и связанные с ней практические реализации, позиционируются как решения, построенные с использованием криптографии и поэтому безопасные. Исходя из этого, возникает ряд вопросов, связанных с оценкой криптографических качеств технологии блокчейн и оценкой информационной безопасности, используемых в данной сфере решений.

Рассматривая технологию блокчейн, с точки зрения обеспечения безопасности, можно выделить следующие уровни:

пользовательский уровень (или уровень приложений),

уровень сетевого взаимодействия,

уровень консенсуса.

На пользовательском уровне подготавливаются данные для включения в распределенный реестр, формируются запросы на чтение и запись к реестру, организуется взаимодействие между отдельными пользователями, осуществляется управление персональными секретными данными, реализуются меры по обеспечению их безопасности.

Криптографической составляющей процесса взаимодействия пользователя с реестром и другими пользователями являются (от примитивов к протоколам):

функции хеширования, использующиеся в схеме ЭЦП, при формировании адреса пользователей, формировании ключевого дерева, формировании ключа из пароля,

схема ЭЦП, может использоваться для контроля целостности, аутентификации отправителя и получателя,

протоколы обмена данными между пользователем и реестром, и между несколькими пользователями.

Уровень сетевого взаимодействия определяет алгоритмы взаимодействия между узлами сети и распространения сообщений между ними. Изначально на данном уровне не предполагали использование криптографических алгоритмов. Однако тенденция развития технологии распределенных реестров ведет к необходимости использования при межсетевом взаимодействии (peer-to-peer communication) криптографических протоколов, обеспечивающих, как минимум, аутентификацию узлов сети, а желательно, и конфиденциальность передаваемой информации.

Уровень консенсуса определяет способы предоставления данных для хранения в распределенном реестре, алгоритмы верификации данных, их записи, чтения и моди-

фикации в реестре. В силу используемых для этой цели алгоритмов их принято называть алгоритмами достижения консенсуса.

Наиболее распространены алгоритмы достижения консенсуса на основе доказательства работы (Proof-of-Work, PoW), доказательства доли (Proof-of-Stake, PoS) и их различные комбинации. Сами алгоритмы и протоколы достижения консенсуса, в общем, не относятся к задачам, решаемым с использованием методов криптографии. Однако, использование в ряде алгоритмов достижения консенсуса криптографических примитивов или математических задач, имеющих практическое применение в криптографии, а также необходимость обеспечения безопасности информации, хранящейся в реестре, позволяет считать алгоритмы достижения консенсуса в блокчейн, криптографическими. И соответственно, рассматривать их с криптографической точки зрения.

Приведенное в предыдущем разделе соответствие между составными частями блокчейн и используемыми криптографическими механизмами позволяет определить следующие подходы к оценке безопасности данной технологии.

На пользовательском уровне и уровне сетевого взаимодействия - в части задач, решаемых с помощью криптографии, можно использовать традиционные модели и методы криптографического анализа.

А именно:

используются стандартные предположения о доступных нарушителю знаниях и методах реализации атак,

решаются традиционные задачи обеспечения безопасности,

используются стандартизированные, криптографические алгоритмы и протоколы.

Следовательно, для оценки криптографических качеств технологии блокчейн можно оперировать традиционными подходами к оценке криптографических качеств, используемых в ней алгоритмов и протоколов.

При этом стоит отметить, что возможность применения ряда популярных криптоатак к алгоритмам, использующимся в технологии блокчейн, практически не оценивалось.

В качестве примера, можно рассмотреть возможность реализации атаки на секретные ключи протокола Bitcoin, с использованием информации, полученной из технических каналов утечки.

В протоколе Bitcoin секретный ключ пользователя однозначно определяет адрес отправителя/получателя денежного перевода или его кошелек. Таким образом, количество наблюдений секретного ключа пользователя, определяющее вероятность данной атаки, пропорционально количеству транзакций, выполненных с данного адреса (кошелька). Хотя в настоящий момент в протоколе Bitcoin рекомендуется использовать для каждой транзакции отдельный ключ, однако данная рекомендация призвана обеспечить анонимность пользователя сети и не связана с защитой от описываемой атаки. При этом ранее используемые ключи не уничтожаются и могут быть использованы пока с адресами, соответствующими данным ключам, связаны транзакции с не использованными входами.

Для защиты от данной атаки можно предложить при проведении любой транзакции переводить все неиспользуемые в ней средства на вновь формируемый адрес и связанный с ним секретный ключ. Однако если каждая операция в блокчейн будет требовать оплаты, такая мера защиты может быть накладной для пользователя.

Для алгоритмов достижения консенсуса модель угроз и нарушителя имеет существенные отличия от моделей, применяемых при анализе криптографических алгоритмов и протоколов. Все протоколы консенсуса существенно зависят от характеристик сети связи. Протоколы консенсуса на основе «доказательства работы» также зависят от

характеристик устройств, верифицирующих данные, включаемые в реестр. Таким образом, при оценке криптографических качеств алгоритмов консенсуса традиционные методы криптографии напрямую неприменимы.

В работе Накамото [1], давшей толчок развитию технологии блокчейн, приведено только эмпирическое доказательство безопасности предлагаемого решения. В дальнейшем был опубликован ряд работ, в которых сделаны попытки формализовать использующиеся в технологии блокчейн, алгоритмы достижения консенсуса и провести их анализ с точки зрения обеспечения безопасности. Выделим ряд работ [3], [4] и [5], появившиеся в последние несколько лет. В работах [3] и [4] авторами была представлена формальная модель ядра протокола Bitcoin, определен ряд фундаментальных свойств протокола. В рамках разработанной модели было формально доказано, что для протокола Bitcoin задача о Византийских генералах решается в случае, когда хеширующая мощность нарушителя не превосходит ½ общей мощности сети. В работе [5] подобные результаты были получены для асинхронных сетей связи.

Заметим, что, исходя из самой их сущности и принципов построения алгоритмов достижения консенсуса, теоретически полученные обоснования стойкости и алгоритмы построения атак сложно верифицируются на практике. При этом, как можно видеть из результатов практического использования технологии блокчейн, большинство угроз безопасности возникает из банальной кражи секретных ключей пользователей.

Таким образом, можно сделать следующие выводы:

при оценке свойств безопасности технологии блокчейн для пользовательского и сетевого уровня можно использовать традиционные подходы к обоснованию безопасности криптографических алгоритмов и протоколов;

возможность применения ряда традиционных криптоатак к технологии блокчейн до настоящего времени не рассматривались, при этом существуют реальные способы их применения на практике;

в настоящее время активно ведутся работы по теоретическому обоснованию стойкости существующих алгоритмов достижения консенсуса для ряда протоколов,

при внедрении технологии блокчейн на практике стоит отдавать предпочтение решениям, имеющим строгое теоретическое обоснование стойкости при условии близости теоретической модели построения протокола к ее практической реализации.

Список литературы

1. S. Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. [2008]. URL: https://bitcoin.org/bitcoin.pdf (дата обращения: 25.03.2017)

2. Satoshi Nakamoto. Bitcoin open source implementation of p2p currency. [2009]. URL: http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source (дата обращения: 25.03.2017)

3. Juan A. Garay, Aggelos Kiayias, Nikos Leonardos. The bitcoin backbone protocol: Analysis and applications. In Elisabeth Oswald and Marc Fischlin, editors, Advances in Cryptology - EUROCRYPT 2015 - 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Sofia, Bulgaria, April 26-30, 2015, Proceedings, Part II, volume 9057 of Lecture Notes in Computer Science, pages 281–310. Springer, 2015.

4. Juan A. Garay, Aggelos Kiayias, Nikos Leonardos. The Bitcoin Backbone Protocol with Chains of Variable Difficulty [2016]. URL:http://eprint.iacr.org/2016/1048.pdf (дата обращения 20.04.2017)

5. Rafael Pass, Lior Seeman, Abhi Shelaty. Analysis of the Blockchain Protocol in Asynchronous Networks. In Jean-Sebastien Coron and Jesper Buus Nielsen, editors, Advances in Cryptology - EUROCRYPT 2017 - 36th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Paris, France, April 30-May 4, 2017, Proceedings, Part II, volume 10211 of Lecture Notes in Computer Science, pages 643–674. Springer, 2017.